IN THE CLAIMS:

Amended claims follow:

1. (Currently Amended) A method for detecting potentially harmful actions on a handheld computer, the method comprising:
monitoring calls to applications resident on the handheld computer;
identifying a code associated with a program initiating said call;
wherein identifying a code comprises identifying a creator code on a handheld computer operating system; and
at least temporarily preventing an action requested by said call from being executed if the identified creator code does not match a creator code associated with data said action is to be performed upon;
wherein the creator code is used to prevent malicious behavior;
wherein at least one of the applications is identified as a trusted application;
wherein the trusted application is not prevented from performing actions even if the creator code associated with the trusted application does not match the creator code associated with the data said action is to be performed upon;
wherein the creator code is a 4-byte value used to tie together a plurality of databases related to an application, at least one database is maintained on the handheld computer using a first creator code that is the same as a second creator code associated with a plurality of patches, the at least one database contains a list of a plurality of the creator codes resident on the handheld computer, and at least one creator code is used to prevent a program from modifying one of the databases with a different creator code.

2. (Original) The method of claim 1 wherein monitoring calls to applications comprises installing a patch on the handheld computer, the patch being operable to intercept calls.

3. (Original) The method of claim 2 wherein installing a patch comprises replacing an API address with a patch address.

4. (Original) The method of claim 2 wherein installing a patch comprises utilizing get trap and set trap commands.

5. (Cancelled)

6. (Cancelled)

7. (Original) The method of claim 1 further comprising receiving data on an infrared port of the handheld computer and installing said data in a temporary database.

8. (Original) The method of claim 7 further comprising asking a user whether to accept said data before loading said data onto the handheld computer.

9. (Original) The method of claim 1 wherein the action requested is a password manipulation.

10. (Original) The method of claim 1 wherein the action requested is deletion of data.

11. (Original) The method of claim 1 wherein the action requested is modification of data.

12. (Original) The method of claim 1 wherein the action requested is manipulation of an operating system.

13. (Currently Amended) A method for detecting potentially harmful actions on a handheld computer, the method comprising:
monitoring requests for action by applications on the handheld computer;
evaluating said requests to determine if said requests may result in potentially harmful behavior to data stored on the handheld computer;
preventing said action from being performed if one of said requests for action is identified as potentially harmful behavior; and
notifying a user of the handheld computer of said potentially harmful behavior;

wherein evaluating said requests comprises comparing a creator code associated with the application requesting said action with a creator code associated with data the action is to be performed upon;
wherein the creator code is used to prevent malicious behavior;
wherein at least one of the applications is identified as a trusted application;
wherein the trusted application is not prevented from performing actions even if said one request is identified as potentially harmful, if requested by the trusted application;
wherein the creator code is a 4-byte value used to tie together a plurality of databases related to an application, at least one database is maintained on the handheld computer using a first creator code that is the same as a second creator code associated with a plurality of patches, the at least one database contains a list of a plurality of the creator codes resident on the handheld computer, and at least one creator code is used to prevent a program from modifying one of the databases with a different creator code.

14. (Previously Amended) The method of claim 13 wherein monitoring the requests for action comprises monitoring API calls.

15. (Cancelled)

16. (Cancelled)

17. (Currently Amended) A computer program product for detecting possibly harmful actions on a handheld computer before the actions are executed, the product comprising:
computer code that monitors calls to applications resident on the handheld computer;
computer code that identifies a code associated with a program initiating said call;
wherein a creator code on a handheld computer operating system is identified;
computer code that at least temporarily prevents an action requested by said call from being performed if the identified creator code does not match a creator code associated with data said action is to be performed upon; and
a computer readable medium that stores said computer codes;
wherein the creator code is used to prevent malicious behavior;
wherein at least one of the applications is identified as a trusted application;

wherein the trusted application is not prevented from performing actions even if the creator code associated with the trusted application does not match the creator code associated with the data said action is to be performed upon;

wherein the creator code is a 4-byte value used to tie together a plurality of databases related to an application, at least one database is maintained on the handheld computer using a first creator code that is the same as a second creator code associated with a plurality of patches, the at least one database contains a list of a plurality of the creator codes resident on the handheld computer, and at least one creator code is used to prevent a program from modifying one of the databases with a different creator code.

18. (Cancelled)

19. (Cancelled)

20. (Currently Amended) A computer program product for detecting possibly harmful actions on a handheld computer before the actions are executed, the product comprising:

computer code that monitors requests for action by applications on the handheld computer;

computer code that evaluates said requests to determine if said requests may result in potentially harmful behavior to data stored on the handheld computer;

computer code that prevents said action from being performed if one of said requests for action is identified as potentially harmful behavior;

computer code that notifies a user of the handheld computer of said potentially harmful behavior; and

a computer readable medium that stores said computer codes;

wherein evaluating said requests comprises comparing a creator code associated with the application requesting said action with a creator code associated with data the action is to be performed upon;

wherein the creator code is used to prevent malicious behavior;

wherein at least one of the applications is identified as a trusted application;

wherein the trusted application is not prevented from performing actions even if the creator code associated with the trusted application does not match the creator code associated with the data said action is to be performed upon;

wherein the creator code is a 4-byte value used to tie together a plurality of databases related to an application, at least one database is maintained on the handheld computer using a first creator code that is the same as a second creator code associated with a plurality of patches, the at least one database contains a list of a plurality of the creator codes resident on the handheld computer, and at least one creator code is used to prevent a program from modifying one of the databases with a different creator code.

21. (Cancelled)

22. (Previously Presented) The method of claim 1, wherein a user has an options of disabling the detection of potentially harmful actions, specifying whether a plurality of databases scanned by a virus scanner are considered trusted if the virus scanner returns a favorable result, requiring a password to turn the handheld computer on, checking data that has entered the handheld computer through an infra-red (IR) port, protecting passwords, and specifying the trusted application.

23. (Previously Presented) The method of claim 1, wherein the temporary prevention of the action requested by said call involves notifying a user that the potentially harmful action has been requested and giving the user a plurality of options selected from the group consisting of: allowing one of the applications to continue with the action, always allowing one of the applications to perform the action, and preventing one of the applications from performing the action.

24. (Previously Presented) The method of claim 4, wherein the get trap and set trap commands identify a pointer to an original address and replace the original address with a new patch address.

25. (Previously Presented) The method of claim 1, wherein an efficient detection of viruses is provided for the handheld computer without sacrificing limited memory of the handheld computer.